UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/760,805	01/17/2001	Satoshi Obana	072982/0214	4394

22428 7590 02/23/2005

FOLEY AND LARDNER
SUITE 500
3000 K STREET NW
WASHINGTON, DC 20007

EXAMINER
ZIA, SYED

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/760,805	**Applicant(s)** OBANA, SATOSHI
	Examiner Syed Zia	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 2004*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. This office action is in response to amendment filed on October 15, 2004. Applicant originally filed Claims 1-20. Applicant currently amended Claims 7, and 17. Presently pending claims are 1-20.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Response to Arguments

3. Applicant's arguments filed October 15, 2004 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1, 7, 14, and 18 applicants argued that the cited prior art (CPA) [Brickell et al. (U. S. Patent 5,867,578)] does not discloses "*a system including structure that allows a partial signature auxiliary data to be generated based on a generated random number and a secret key of an owner of a mobile agent, where the partial signature auxiliary data ... calculated by the remote hosts,* and cited prior art do not disclose "*a partial signature combining process for* *receiving one or more partial signatures ...by use of a secret key of the owner of the mobile agent*".

This is not found persuasive. The system of Brickell et al. teaches and describes a system and method of multi-step digital signature having a distributed root certifying authority. Messages received at the root certifying authority are distributed to root certifying authority members who attach *partial signatures* to the message using root key fragments, and enables alteration fragments of private key without need for changing public key.

In the system and method provided, the system adapts to system events such as the addition or removal of key fragment holders, the need to modify key fragments, etc., by changing key fragments, and the signing protocol for certifying authority member is changed by the input instructions.

Therefore, the system of cited prior art describes and a provide a signature calculation system by use of a agent, by which information that can be generated by the owner of the agent only is carried by the agent in a form that can not be analyzed by a single remote host, and thereby a digital signature can be calculated for signature target data by use of a secret key (col.3line 45 to col.4line 62)

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that the system of cited prior arts does teach or suggest the subject matter broadly recited in independent Claims 1, 9, and 17 and in subsequent dependent Claims. Accordingly, rejections for claims 1-24 are respectfully maintained.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Brickell et al. (U. S. Patent 5,867,578).

3. Regarding Claim 1 Brickell teach and describe a signature calculation system by use of a mobile agent (Fig.1-3), comprising:

a mobile agent for calculating a digital signature of the owner of the mobile agent; a base host of the mobile agent from which the mobile agent starts moving in a network; and remote hosts in the network which can be visited by the mobile agent (col.5 line 12 to line 47), wherein: the base host includes:

an agent execution environment for letting the mobile agent execute its program code; a random number generation means for generating random numbers; a partial signature auxiliary data generation means to which the random numbers generated by the random number generation means and a secret key of the owner of the mobile agent are inputted and which generates partial signature auxiliary data for distributing the information of the secret key of the owner of the mobile agent to the remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of the digital signature of the owner of the mobile agent are calculated by remote hosts; and a public key cryptography calculation means for conducting encryption and signature calculation for the partial signature auxiliary data generated by the partial signature auxiliary data generation means (col.5 line 12 to col.7 line 34), and

each remote host includes: an agent execution environment for letting the mobile agent execute its program code; a partial signature calculation means to which signature target data, data which have been carried by the mobile agent and a secret key of the remote host are inputted and which calculates a partial signature which is necessary for the calculation of the digital signature of the owner of the mobile agent; a partial signature combining means to which one or more partial signatures calculated by one or more remote hosts are inputted and which outputs the digital signature calculated for the signature target data by use of the secret key of the owner of the mobile agent; and a public key cryptography calculation means for conducting encryption and signature calculation for the partial signature calculated by the partial signature calculation means (col.7 line 36 to col.9 line 9), and

the mobile agent, which started from the base host carrying the partial signature auxiliary data and which is arbitrarily presented with the signature target data by a remote host, stores the signature target data if the mobile agent determined to write the digital signature for the signature target data by use of the secret key of the owner of the mobile agent, and thereafter visits k (k: security parameter) remote hosts and carries the partial signatures calculated by the remote hosts to the remote host that presented the signature target data, at which the digital signature for the signature target data by use of the secret key of the owner of the mobile agent is obtained from the partial signatures calculated by the k remote hosts (col.11 line 11 to col.16 line 25).

4. Regarding Claim 7 Brickell teach and describe signature calculation system by use of a mobile agent (Fig.1-3) comprising:

a mobile agent for calculating a digital signature of the owner of the mobile agent; a base host of the mobile agent from which the mobile agent starts moving in a network; and remote hosts in the network which can be visited by the mobile agent (col.5 line 12 to line 47), wherein: the base host includes:

an agent execution environment for letting the mobile agent execute its program code; a random number generation means for generating random numbers; a partial signature auxiliary data generation means to which the random numbers generated by the random number generation means are inputted and which generates a new secret key and a new public key corresponding to the newly generated secret key and generates partial signature auxiliary data for distributing the information of the newly generated secret key to the remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of the digital signature of the owner of the mobile agent are calculated by remote hosts; and generating a digital signature for partial signature auxiliary data for secret key of the owner of a mobile agent, and a public key cryptography calculation means for conducting encryption and signature calculation for the partial signature auxiliary data generated by the partial signature auxiliary data generation means (col.5 line 12 to col.7 line 34, and col.14 line 9 to line 40),

and each remote host includes: an agent execution environment for letting the mobile agent execute its program code; a partial signature calculation means to which signature target data, data which have been carried by the mobile agent and a secret key of the remote host are inputted and which calculates a partial signature which is necessary for the calculation of the digital signature of the owner of the mobile agent; a partial signature combining means to which one or more partial signatures calculated by one or more remote hosts are inputted and which outputs the digital signature calculated for the signature target data by use of the newly generated secret key; and a public key cryptography calculation means for conducting encryption and signature calculation for the partial signature calculated by the partial signature calculation means (col.7 line 36 to col.9 line 9), and

the mobile agent, which started from the base host carrying the partial signature auxiliary data and which is arbitrarily presented with the signature target data by a remote host, stores the signature target data if the mobile agent determined to write the digital signature for the signature target data by use of the newly generated secret key, and thereafter visits k (k: security parameter) remote hosts and carries the partial signatures calculated by the remote hosts to the remote host that presented the signature target data, at which the digital signature for the signature target data by use of the newly generated secret key is obtained from the partial signatures calculated by the k remote hosts (col.11 line 11 to col.16 line 25).

5. Regarding Claim 13 Brickell teach and describe computer-readable record medium storing a program for instructing a computer of a base host of a mobile agent to execute (Fig.1-3):

an agent execution process for letting the mobile agent execute its program code; a random number generation process for generating random numbers; a partial signature auxiliary data generation process for receiving the random numbers generated in the random number generation process and a secret key of the owner of the mobile agent as input data and generating partial signature auxiliary data for distributing the information of the secret key of the owner of the mobile agent to remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of a digital signature of the owner of the mobile agent are calculated by remote hosts; and

a public key cryptography calculation process for conducting encryption and signature calculation for the partial signature auxiliary data generated in the partial signature auxiliary data generation process (col.5 line 12 to col.7 line 34).

6. Regarding Claim 14 Brickell teach and describe computer-readable record medium storing a program for instructing a computer of a remote host to execute (Fig.1-3):

an agent execution process for letting a mobile agent execute its program code; a partial signature calculation process for receiving signature target data which has been arbitrarily presented to the mobile agent by a remote host, data which have been carried by the mobile agent, and a secret key of the remote host as input data, and calculating a partial signature which is necessary for the calculation of a digital signature of the owner of the mobile agent for the signature target data; a partial signature combining process for receiving one or more partial signatures calculated by one or more remote hosts as input data and outputting the digital signature calculated for the signature target data by use of a secret key of the owner of the mobile agent; and a public key cryptography calculation process for conducting encryption and signature calculation for the partial signature calculated in the partial signature calculation process (col.7 line 36 to col.9 line 9).

7. Regarding Claim 17 Brickell teach and describe computer-readable record medium storing a program for instructing a computer of a base host of a mobile agent to execute (Fig.1-3):

an agent execution process for letting the mobile agent execute its program code; a random number generation process for, generating random numbers; a partial signature auxiliary data generation process for receiving the random numbers generated in the random number generation process as input data, generating a new secret key and a new public key corresponding to the newly generated secret key, and generating partial signature auxiliary data for distributing the information of the newly generated secret key to remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of a digital signature of the owner of the mobile agent are calculated by remote hosts, and generating a digital signature for partial signature auxiliary data for secret key of the owner of a mobile agent; and a public key cryptography calculation process for conducting encryption and signature calculation for the partial signature auxiliary data generated in the partial signature auxiliary data generation process (col.5 line 12 to col.7 line 34, col.14 line 9 to line 40).

8. Regarding Claim 18 Brickell teach and describe computer-readable record medium storing a program for instructing a computer of a remote host to execute (Fig.1-3):

an agent execution process for letting a mobile agent execute its program code; a partial signature calculation process for receiving signature target data which has been arbitrarily presented to the mobile agent by a remote host, data which have been carried by the mobile agent, and a secret key of the remote host as input data, and calculating a partial signature which is necessary for the calculation of a digital signature of the owner of the mobile agent for the signature target data; a partial signature combining process for receiving one or more partial signatures calculated by one or more remote hosts as input data and outputting the digital signature calculated for the signature target data by use of the newly generated secret key; and a public key cryptography calculation process for conducting encryption and signature calculation for the partial signature calculated in the partial signature calculation process (col.7 line 36 to col.9 line 9).

9. Claims 2-3, 5, 8, 9,11, 15, and 19 are rejected applied as above rejecting Claims 1, 7, 14, and 18. Furthermore, Brickell teach and describe a signature calculation system by use of a mobile agent, wherein

one or more components of the remote host selected from the partial signature calculation means, the partial signature combining means and the public key cryptography calculation means are implemented by program code of the mobile agent (col.18 line 55 to col.19 line 38);

the partial signature auxiliary data generated by the partial signature auxiliary data generation means include cipher texts (G; M;) (1 [less than or equal] i < k) which are obtained by encrypting random numbers ri (1 [less than or equal] i < k) that satisfy a predetermined relationship with the secret key of owner of the mobile agent by use of ElGamal cryptosystem public keys yi (1 [less than or equal] i < k); and the digital signature calculated for the signature target data is an RSA digital signature; and one or more components of the remote host selected from the partial signature calculation means, the partial signature combining means and the public key cryptography calculation means are implemented by program code of the mobile agent (col.9 line 12 to col.11 line 10, and col.14 line 57 to col.16 line 25).

10. Claims 4, 6, 10, 12, 16 and 20 are rejected applied as above rejecting Claims 3, 5, 9, 11, 15, and 19. Furthermore, Brickell teach and describe a signature calculation system by use of a mobile agent, wherein

signatures calculated for the random numbers ri (1 [less than or equal] i < k) by use of the secret key of the owner of the mobile agent are added to the partial signature auxiliary data carried by the mobile agent (col.3 line 66 to col.4 line 28).

the partial signature combining means of the remote host that presented the signature target data calculates the digital signature for the signature target data by obtaining the product (mod p X q (p, q: prime number of approximately 512 bits)) of the partial signatures calculated by the k remote hosts (col.9 line 11 to col.12line 38).

signatures calculated for the random numbers ri (1 [less than or equal] i < k) by use of a secret key of the owner of the mobile agent, a signature calculated for the newly generated public key by use of the secret key of the owner of the mobile agent, and the newly generated public key are added to the partial signature auxiliary data carried by the mobile agent (col.3line 66 to col.4 line 28);

in the partial signature combining process, the digital signature for the signature target data is calculated by obtaining the product (mod px q (p, q: prime number of approximately 512 bits) of the partial signatures calculated by the one or more remote hosts (col.9 line 11 to col.12 line 38).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

sz
February 10, 2005

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER